Article from **Dealer Magazine** (http://www.imakenews.com/dealercomm1/e_article001010072.cfm?x=b11,0,w)

February 5, 2008

The Red Flags solution

So far in my discussion of the Red Flags Rule, I listed the potential red flags that the Feds suggest you should address in your final policy, as well as delineated the potential red flags into an electronic solution and those that require a manual process. Today, I will discuss how a dealer can comply with the Rule.

The Feds identified 26 red flags as potential indicators of identity theft. The Rule requires a dealer to establish a process to ensure that each transaction is reviewed against all red flags a dealer identifies in his risk assessment. Whenever one of the red flags is tripped, the dealer must take action before proceeding with the sale.

Since the potential red flags can be picked up either electronically or through a manual review, a dealer must have a multi-pronged approach to complying with the Rule.

First the Six Elements of a Compliance Program
The Feds require six elements be present for a dealer to be in compliance with the Red Flags Rule:
1. Identify a compliance officer
2. Conduct a risk assessment
3. Develop a policy
4. Provide employee training
5. Conduct periodic audits
6. Provide an annual report to the dealership owner(s)

Identifying Red Flags in Transactions
For the electronic piece, consider checking out the numerous vendors who will have solutions on display this weekend at the NADA convention. The ones I've reviewed have solid algorithms in place to provide a dealer with the ability to determine if one of the red flags is present in a transaction. They provide a dealer with a report or warning that a red flag is present. It is then incumbent on the human to recognize the warning and take action.

Other red flags can only be ferreted out by human observation and intervention. For example, comparing the customer's identification to the customer must be completed by a human. No amount of electronic sophistication can take the place of the manual observations of potential red flags.

Humans Need Training
Regardless of whether a red flag is tripped through an electronic algorithm or through human observation, action must be taken by humans.

The first part to any viable solution, after the process is in place, is to train all employees. This training must emphasize to the employees the seriousness of identity theft, the damage it does to the victim and the employee's responsibility to be vigilant in the detection of identity theft.

An effective training program will include the initial training of all employees, the training of all new hires upon ascension and a regularly scheduled follow-up training of all employees.

Humans Need Verification
Once the program is in place, and the employees have been trained, a dealer must have an audit process in place to continuously monitor the program's effectiveness and that all employees have been trained and are following the program. The audit must contain steps to review and

test both electronic and manual processes. Any shortcomings uncovered during the audit are to be corrected, documented and appropriate changes made to the program's procedure.

Government Wants Accountability
The Feds added an additional element to the five elements it established for the Safeguards Rule. The Red Flags Rule requires that an annual report be completed and delivered to the dealership owner or Board of Directors detailing the program's effectiveness and sufficiency. Regardless of the solution a dealer adapts to fulfill the electronic portion of the Rule, the report will need to be completed by a human, preferably the same one that conducted the audits.

Gil Van Over is the President and founder of gvo3 & Associates, a nationally recognized F&I, Sales and Red Flag Rule compliance consulting and training firm (www.gvo3.com).